(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 700 023 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
06.03.1996 Bulletin 1996/10

(51) Int. Cl.[6]: **G07F 7/08**

(21) Application number: **95202353.9**

(22) Date of filing: **31.08.1995**

(84) Designated Contracting States:
AT BE CH DE DK ES FR GB GR IE IT LI LU NL PT SE

(30) Priority: **31.08.1994 NL 9401406**

(71) Applicant: **Koninklijke PTT Nederland N.V.**
NL-2509 CH The Hague (NL)

(72) Inventor: **Felken, Albertus**
NL-1186 TD Amstelveen (NL)

(54) Payment system with improved integrity

(57) Improved integrity of a payment system for the payment of services or goods, for example telephone facilities, making use of electronic payment cards. In any session to increase the card balance, a "flag" is placed ("1") on the payment card which indicates that said session must not be interrupted. After completion, the flag is removed again ("0"). A session to pay for the product or the service or to increase the balance can only be set up if the flag is absent ("0") indicating that the last session to increase the balance was correctly completed. If, on the other hand, the flag is still "1" at the start of a session, a correction routine is first carried out in which the previous session to increase the balance is correctly concluded after all. In order to prevent the flag being removed by fraud, it can be removed only by the central system (PSTN/ABS) by means of an authorized instruction.

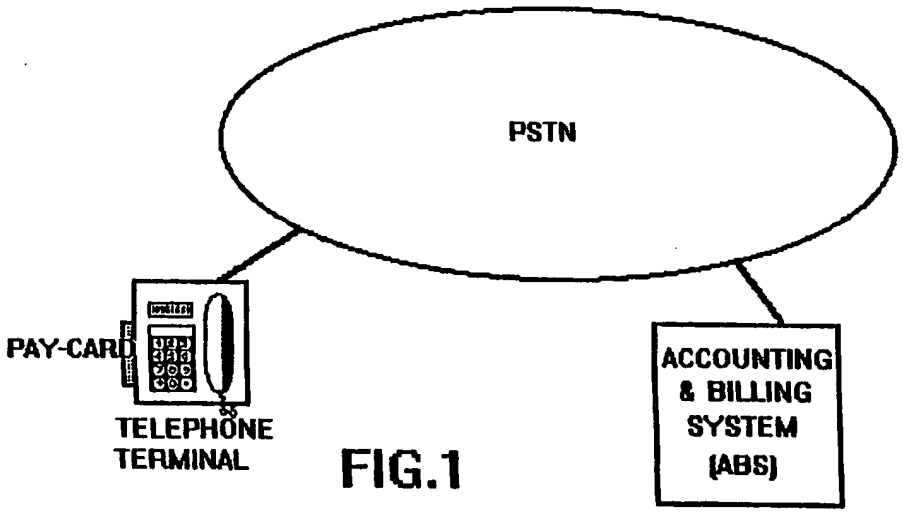

FIG.1

EP 0 700 023 A1

Printed by Rank Xerox (UK) Business Services
2.9.11/3.4

3/22/06, EAST Version: 2.0.3.0

Description

BACKGROUND OF THE INVENTION

The invention relates to a payment system in which use is made of electronic payment cards, in particular "chip cards" or "smart cards". Under consideration in the present application are, in particular, payment cards which can be used for paying the call costs in public telephone terminals. However, other services and goods can also be paid for in this way. This development is in fact referred to as "electronic purse". Under consideration in this connection is the payment of generally none too large amounts by means of electronic payment cards on which a balance is entered beforehand. Payment takes place by reducing the balance on the card. Of course, measures have to be taken in order to arrange for the reduction in balance to benefit the supplier; systems for this purpose are still being developed and tests are taking place in that field. To place an initial balance on the card and add to the balance later, there must be an infrastructure of terminals and the like if this form of payment is to be accepted. It appears possible to use the public telephone terminals for this purpose. They can then therefore act as "charging station" for electronic payment cards. Of course, the public telephone terminals remain suitable as means for conducting telephone calls and offering any other telecommunication facilities via the downstream central telephone system or telecommunication system. Payment of said calls and any other facilities may, at the same time, take place by means of the "electronic purse". Although the payment of telephone/telecommunication costs, in particular, is considered below, it is emphasized that the invention explained below is not limited thereto and is equally applicable in the payment for other services or goods by means of an "electronic purse". The "charging" of payment cards does not per se have to take place via telephone terminals either, but can equally well take place via other terminals, for example terminals which are now used for issuing cash ("cash points").

After a payment card has been provided with an initial balance, that balance is reduced by the telephone terminal in accordance with the rate for the telephone costs. The provision of an initial balance and the topping up of said balance after the passing of time can also be carried out via the telephone terminal. To do this, connection has to be made to a central administration system which, on the one hand, enters the amount desired by the user on the card and, on the other hand, ensures that the amount can be received, for example by sending an account to the user or via (after authorization) electronic reduction of the balance of a bank account belonging to the user.

The measures proposed according to the present invention are intended to combat errors and frauds in the processes mentioned (the use/payment process) and the "balance process").

SUMMARY OF THE INVENTION

The essence of the invention is that a "flag" is placed on the payment card during each balance process throughout the entire process time in order to indicate that the payment card is occupied with an indivisible action, i.e. a process which cannot be interrupted. After said indivisible action has taken place, the flag is removed again. The placing and removal of a flag takes place by writing a certain first symbol (for example, "1") or second symbol (for example, "0") into a certain memory location of the payment card. The exploitation process and payment process (the use of the telephone facilities) can only be started after it has been confirmed that there is no flag at said certain memory location, which means that the last balance process was correctly concluded. If there is in fact a flag, no connection to the telephone system is set up. Instead thereof, a balance session is set up in which the incorrectly concluded previous session is repeated or is continued and correctly concluded after all on the basis of the information still present in the administration system.

In order to prevent the flag being capable of being removed by fraud, for example by means of a PC and a card terminal (under consideration is the situation where the payment card is pulled out of the terminal during the balance process at the instant when the balance on the card has already been increased while preparation of the invoice (or automatic debit instruction) has not yet taken place) provision is preferably made that the flag can be removed only by the central system which is concerned with increasing the balance. The code signal for removing the flag is therefore preferably also presented to the payment card provided with a cryptographic code which the central system denotes as the origin of said code signal (message authentication code, MAC). If this appears to be correct, the code signal is converted into an instruction to replace the first symbol ("1", "flag up") into the second symbol ("0", flag down"). Preferably, if EEPROM cards are used, various instructions are used to set up the flag and to remove it. For the first action ("0" → "1"), the instruction "WRITE" is used and for the second action ("1" → "0"), the instruction "MODIFY" is used. The

3/22/06, EAST Version: 2.0.3.0

difference is:

bit in buffer	WRITE		bit in buffer
0	0	→	0
1	0	→	1
0	1	→	1
1	1	→	1
bit in buffer	**MODIFY**	**→**	**bit in buffer**
0	0	→	0
1	0	→	0
0	1	→	1
1	1	→	1

EXEMPLARY EMBODIMENTS

The invention is discussed in greater detail below with reference to a diagrammatic representation of a card telephone system in Figure 1 and four diagrams in Figures 2 - 5.

Figure 1 shows a telephone network (PSTN) to which a telephone terminal is connected. Payment of telephone costs takes place by periodically reducing the balance of an electronic payment card. The balance of said card can be increased by inserting the card into the terminal. Connection is made to an "Accounting & Billing" system (ABS) connected to the PSTN in a menu-controlled dialog with the terminal (via the keyboard and display window of the terminal). After a balance desired by the user has been entered (for which the user receives an invoice from the ABS), the payment card can be used to start a telephone session with the PSTN, the costs of which are paid by periodically debiting the balance.

The diagram of Figure 2 shows diagrammatically the protocol which is carried out after a user has inserted his payment card into the terminal.

After the card has been inserted into the terminal and the identity has been established and authorized (like further protocol details, this is not indicated in the figures), the "flag" of the payment card is read. This normally has (in this example) the value "0": "flag down". If the flag is down, the setting up of a telephone connection can be started, which is illustrated in Figure 3. In place thereof, an action can also be started to increase the card balance, see Figure 4. If the flag has the value "1" ("flag up"), something is not in order and an error routine is first processed; this is shown in Figure 5.

Figure 3 shows the routine for setting-up and payment of a telephone call by means of the card balance. In this process, whether the initial balance is sufficient is first investigated, the connection is set up and periodically an amount P is deducted from the card balance. As soon as the balance is insufficient, the connection is interrupted.

Figure 4 shows the routine for increasing the card balance. The first action is to raise the flag ("1"). This is an indication that the "RAISE CREDIT" routine is in progress; only at the end of the latter is the flag lowered ("0"). The amount by which the balance has to be increased is entered via the keyboard of the terminal (the same one as that with which telephone connections can be dialled). After the value of the flag has been read for the purpose of security (it ought to be "1"), the card balance is read. Connection is also made to ABS (via the telephone network). The card balance and the amount with which the card balance has to be topped up is now transmitted by the terminal to the ABS and registered at the latter (CAR). The terminal then instructs the payment card to increase the balance by the amount; the card transmits the new balance to the ABS via the terminal. The amount entered is compared in the ABS with the difference between the new and the old card balance and, in the event of agreement, the invoice is prepared for the user. The registration of the old card balance in the ABS and the amount entered by the user are then erased. Finally, the flag on the payment card is lowered again. The instruction to do this is received from the ABS using "message authentication" by means of a cryptographic "message authentication code" (MAC). This is checked in the payment card, after which the flag is set by means of a MODIFY instruction to "0". The payment card is programmed in such a way that the MODIFY instruction can be carried out only together with a correct MAC. Use of MACs is generally known, inter alia from "Electronic banking using smartcards", SMART CARD '90, Int. Exh. and Conf. PLF Commun., vol. 2, 1990, pages M1-8, or from the book entitled "Security for Communication Networks" by Davis and Price.

3/22/06, EAST Version: 2.0.3.0

Figure 5 shows the routine which is processed if, after the payment card has been inserted, it is found that the flag is raised. This indicates that an earlier action to increase the card balance has not been correctly terminated. The incorrectly processed previous action is now correctly terminated by the routine from Figure 5.

First of all (lines 50 - 51) it is investigated whether the registration (made during said previous action) of the old card balance and the amount by which the balance had to be increased (CAR) still exists in the ABS. If this was erased in the previous action, the only action which has to be carried out is to reset the flag. It may be assumed that only the resetting of the card flag has been omitted in the incorrectly concluded action (lines 52 - 53).

If the CAR still exists (lines 54 - 55), it is investigated whether the registered card balance is or is not equal to the present card balance (line 56).

If the present card balance is greater than the registered card balance in the CAR, it may be assumed that during the previous session the card balance has in fact been increased but that no account thereof has been prepared. In that case, the account is now made up, the CAR is erased and the flag is reset (lines 57 - 59).

If the present card balance is equal to the card balance registered in the CAR, the previous attempt to increase the balance is now processed, namely on the basis of the amount, known from the CAR, by which the balance had to be increased. The card balance is now increased, the account is prepared, the CAR is erased and the flag is reset (lines 60 - 66). After an incorrect session to increase the card balance was signalled by detection of the flag and said error was then corrected, the planned session for which the choice was already made (see Figure 2, lines 12 - 14) can be started after all (line 67).

REFERENCES

None

Claims

1. Payment system in which, during a balance process comprising an increase in the balance of an electronic payment card, said payment card is inscribed with a first symbol which, after completion of said balance process, is changed into a second symbol.

2. Payment system in which, during a payment process comprising the payment for a product or a service by reducing the balance of the payment card, the presence of the first symbol or the second symbol is detected and in which the payment process is carried out only if the second symbol is present.

3. Payment system according to Claim 1, in which, at the beginning of the balance process, the presence of the first or the second symbol is detected and, if the second symbol is present, said second symbol is changed into the first symbol, after which the balance process is carried out, while if the first symbol is present, indicating that a previous balance process was interrupted, the interrupted previous balance process is completed or repeated.

4. Payment system according to Claim 2, in which, at the beginning of the payment process, the presence of the first or the second symbol is detected and the payment process is executed only if the second symbol is present, while if the first symbol is present, indicating that a previous balance process was interrupted, the interrupted previous balance process is completed or repeated before executing the payment process.

5. Payment system according to Claim 3, in which electronic payment cards are connected via a decentralized terminal to a central system (PSTN/ABS) which, after completion of the balance process, sends a signal to the terminal, as a result of which the first symbol is changed into the second symbol on the payment card.

6. Payment card according to Claim 5, in which the terminal changes the second symbol on the payment card into the first symbol at the beginning of the balance process.

7. Payment process according to Claim 5, in which the payment cards comprise an EEPROM and the changing of the first symbol into the second symbol takes place by means of a MODIFY instruction code.

8. Payment system according to Claim 6, in which the payment cards comprise an EEPROM and the changing of the second symbol into the first symbol takes place by means of a WRITE instruction code.

9. Payment system according to Claim 1, in which, to carry out the balance process, the electronic payment card is connected via a decentralized terminal and a central telephone system or telecommunication system (PSTN) to an administration system (ABS).

3/22/06, EAST Version: 2.0.3.0

10. Payment system according to Claim 9, in which said decentralized terminal is a telephone terminal or telecommunication terminal.

11. Payment system according to Claim 2, in which the electronic payment card can be connected to the decentralized telephone terminal or telecommunication terminal of a central telephone system or telecommunication system (PSTN) and in which use can be made of the telephone facilities or telecommunication facilities of said telephone system or telecommunication system at any rate at least insofar as payment of said facilities takes place by reducing the balance of said payment card, only after detection of the second symbol.

3/22/06, EAST Version: 2.0.3.0

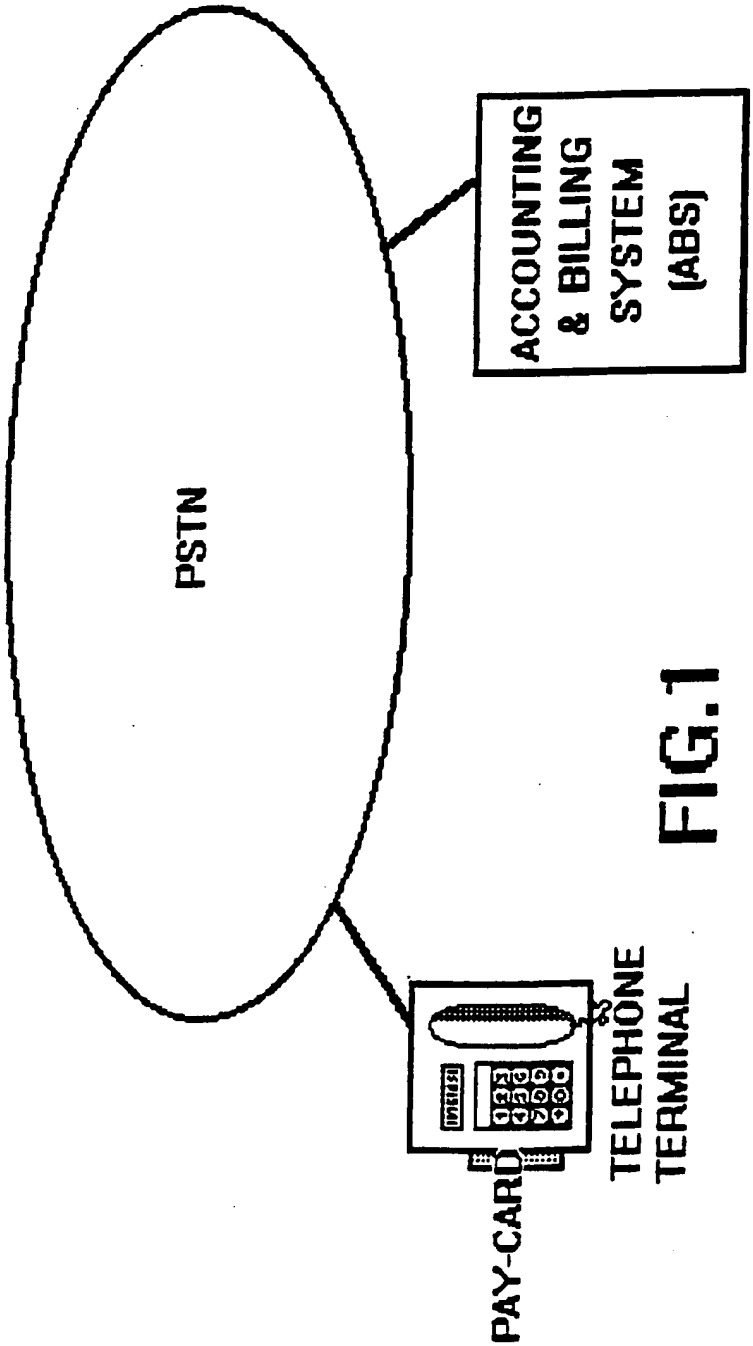

FIG.1

3/22/06, EAST Version: 2.0.3.0

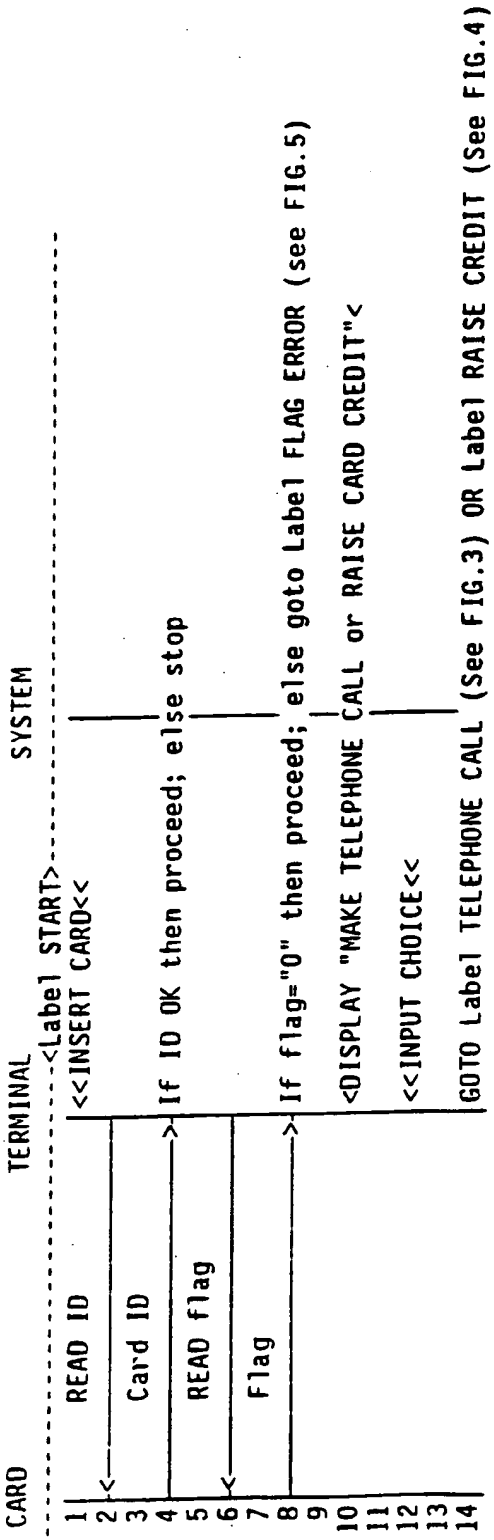

FIG.2

3/22/06, EAST Version: 2.0.3.0

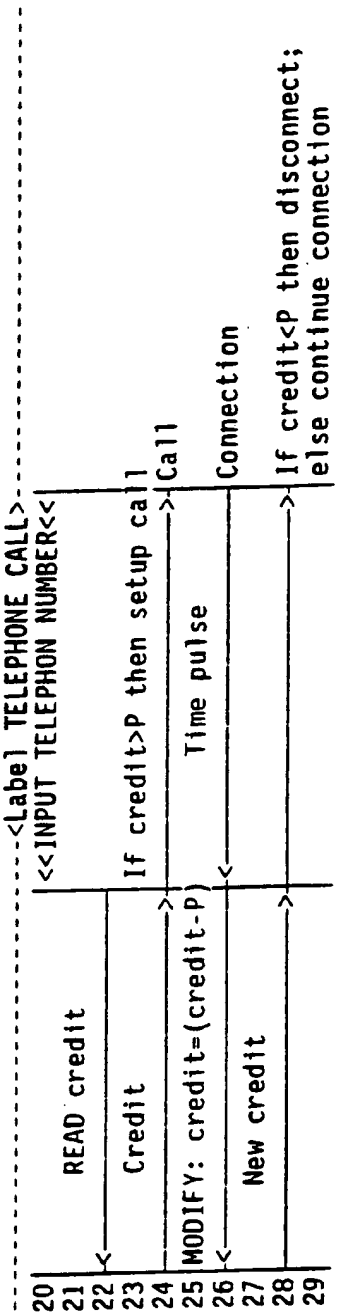

FIG.3

3/22/06, EAST Version: 2.0.3.0

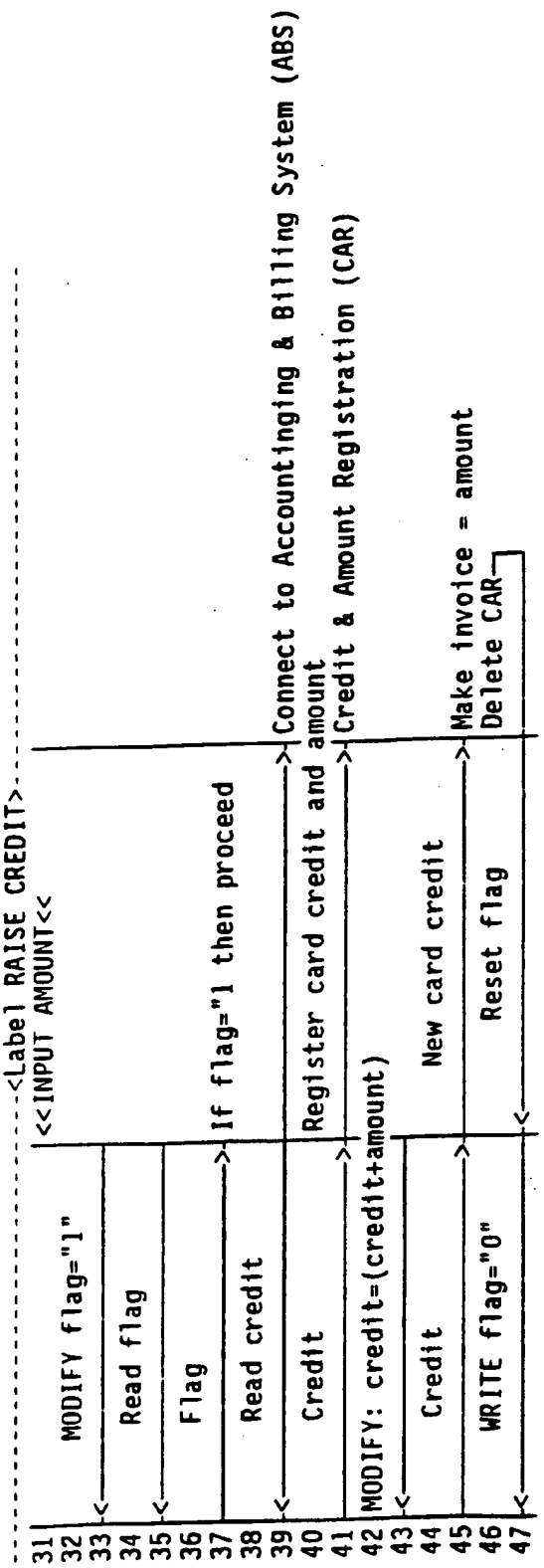

FIG.4

3/22/06, EAST Version: 2.0.3.0

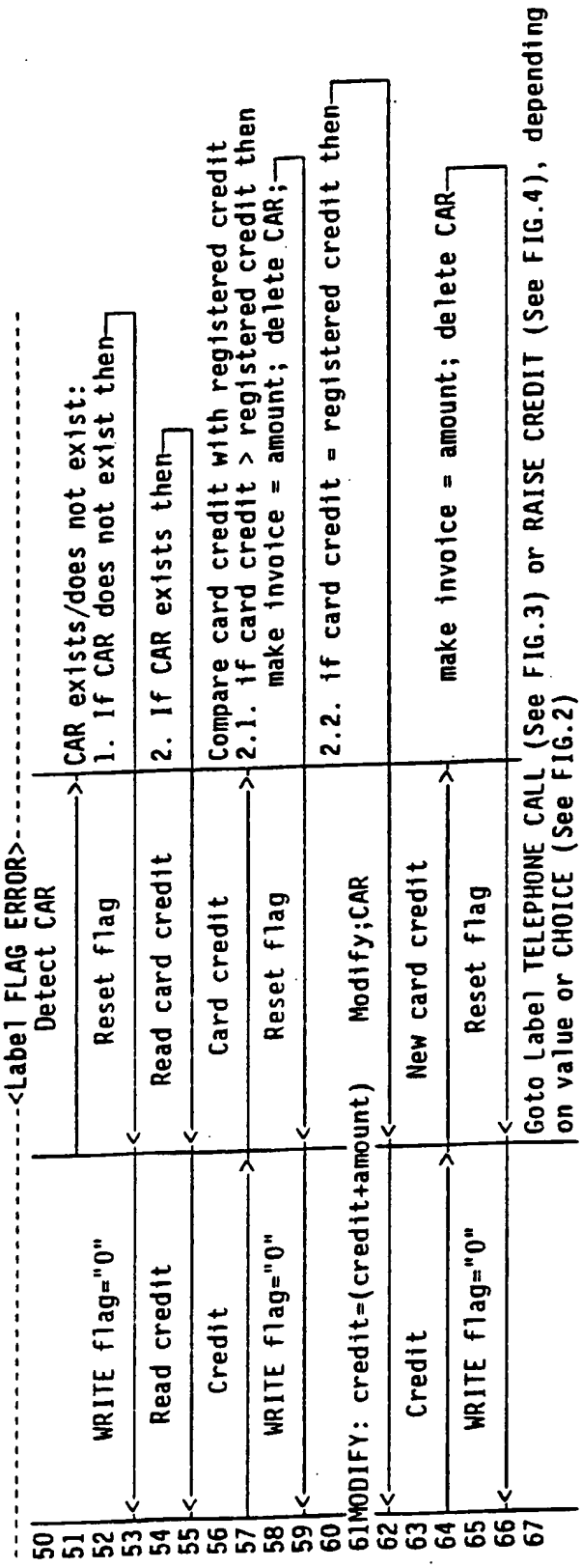

FIG.5

3/22/06, EAST Version: 2.0.3.0

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 95 20 2353

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
X A	WO-A-89 02140 (MARS) * abstract; claims; figures * * page 13, line 11 - page 20, line 6 * * page 20, line 20 - page 21, line 3 *	1,6,8 2-5,7,9-11	G07F7/08
A	FR-A-2 689 662 (GEMPLUS CARD INTERNATIONAL)	1,2,4,6,8	
A	US-A-4 877 945 (K. FUJISAKI) * the whole document *	1-4,6-8	
A	DE-A-42 30 866 (VENTURE ENGINEERING) * abstract; claims; figures 1,2,13-15 *	1,5,9-11	
A	NL-A-9 200 857 (RIJKSWATERSTAAT)		
A	EP-A-0 563 997 (TOSHIBA)		

TECHNICAL FIELDS SEARCHED (Int.Cl.6)

G07F
G06K

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	22 December 1995	David, J

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

3/22/06, EAST Version: 2.0.3.0